UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/670,298	09/26/2003	Andrea Klaes	SRE-0003-US	6494

36183 7590 08/08/2007

PAUL, HASTINGS, JANOFSKY & WALKER LLP
P.O. BOX 919092
SAN DIEGO, CA 92191-9092

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
08/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/670,298	KLAES, ANDREA	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 May 2007 and 26 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 16 May 2007, has been received, entered into the record, respectfully and fully considered.

2. As a result of the amendment, claims 1, 12, 19 and 22 have been amended. Claims 1-30 are now presented for examination.

3. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As per **claims 1, 12 and 22**, the Applicant amended the claims by adding proxy loghost and the central loghost are remote from each other and in communication with each other over a network. The examiner respectfully and carefully reviews the original disclosure. However, according to Applicant's disclosure on par. [0017], it discloses "**both proxy and central loghosts as independent modules that can run on the**

same system". "Independent modules that can run on the same system" are not same as "remote from each other". On page 9 of the remark, the Applicant states the supporting of this amendment is in par. [0014]-[0015] and fig. 1. The examiner found no support in the par. [0014]-[0015] at all of this new limitation. Instead, in par. [0014]-[0015], contrary to Applicant's remark and amended claims, the Applicant discloses "A central loghost 100 is in communication with a network 150". Please note "A central loghost 100 is in communication with a network 150" is not the same as proxy loghost and the central loghost are in communication with each other over a network. Further, in par. [0015], the Applicant describes fig. 1 "...log files from substantially all of the resources 170 that generate log files, and that generate log files, and that may be in communication with a respective network 150, are forwarded...to a corresponding proxy loghost 160". Furthermore, the Applicant discloses in fig. 1, a network connected between proxy loghost 160 and central Loghost, but that does not mean proxy loghost 160 and central loghost are remote from each other. Given a well known example in the art, two computers under the same system connected through a network and they can be next to each other or in a very close proximity, not necessiarly be remote from each other even though they are connected by a network. Therefore, fig. 1 does not support the new claim limitations as well.

Furthermore, **claim 12** has another new limitation "the central loghost receiving the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing **the log files and the events**...". However, in the par. [0015] of the

instant application, the Applicant discloses, "...to a corresponding proxy loghost 160...these log files are then analyzed and "events" are generated. The events are then forwarded to central loghost 100 for further analysis". It appears to the examiner that proxy loghost analyzes the log files and the central loghost 100 analyzes the event. Therefore, the new limitation has no support in the original disclosure if there are proxy loghosts in the enterprise. Additionally, the Applicant discloses in par. [0031], "In some cases an enterprise may be sufficiently small as to **not** justify implementing proxy loghosts. In such a case...and both generate and analyze events." Please note in this instance according to the original disclosure, there are **no** proxy loghosts are in the system. In the claim, a plurality of proxy loghosts are being recited. Thus, the new limitation has no support in the original disclosure at all.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

6. Claims 12-21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per **claim 12**, "the central loghost receiving the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing **the log files and the events**...". However, in the par. [0015] of the instant application, the Applicant

discloses, "...to a corresponding proxy loghost 160...these log files are then analyzed and "events" are generated. The events are then forwarded to central loghost 100 for further analysis". It appears to the examiner that proxy loghost analyzes the log files and the central loghost 100 analyzes the event. Therefore, the new limitation has no support in the original disclosure if there are proxy loghosts in the enterprise. Additionally, the Applicant discloses in par. [0031], "In some cases..small as to not justify implementing proxy loghosts. In such a case...and both generate and analyze events." Please note in this instance according to Applicant's original disclosure, there are **no** proxy loghosts are in the system. In the claim, a plurality of proxy loghosts are being recited. *In re Wands, 858 F. 2d 731, 737, 8 USPQ2D 1400, 1404 (Fed. Cir. 1998)*. Therefore, the amended claim limitation in claim 12 is contradicted with the Applicant's original disclosure, which is not enabling.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 1-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In claims 1-11, a "computer-implemented system" is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. On page 5, par. [0017] of the specification, the Applicant defined "both proxy and central loghosts are independent modules". Also, on page 4, par. [0015] of the specification, the Applicant defined "resources" is to be constructed broadly as "any system that may be connected to (or operating within) a given network and that generates log files....many enterprise software applications...and the like generate log files....". All other claim limitations such as software adapters, module, log files are software. As such, it believes that the system of claims 1-11 are reasonably interpreted as functional descriptive material, per se.

In claims 12-21, a "computer-implemented system" is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. On page 5, par. [0017] of the specification, the Applicant defined "both proxy and central loghosts are independent modules". Also, on page 4, par. [0015] of the specification, the Applicant defined "resources" is to be constructed broadly as "any system that may be connected to (or operating within) a given network and that generates log files....many enterprise software applications...and the like generate log files....". All other claim limitations such as software adapters, module, log files are software. As such, it believes that the system of claims 12-21 are reasonably interpreted as functional descriptive material, per se.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. Claims 1-7, 9-17, 19-28 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar et al. (U.S. Patent No. 7,127,743).

As per **claim 1**, Khanolkar et al. discloses a computer-implemented monitoring/intrusion detection system (e.g. abstract), comprising:

a central loghost ("an event manager" disclosed in the abstract corresponds to Applicant's central loghost),

at least one proxy loghost ("syslog listener and an event parser" disclosed in col. 7, lines 45-46 corresponds to Applicant's proxy loghost) remote from the central loghost and ("..is a distributed network of monitoring systems, each accessible to a central

console ...**remote** from the source computer system...in the distributed network" – e.g. col. 3, lines 3-8, "...As used herein, "**in communication with**" and "**coupled**" include **direct and indirect** (i.e., through an intermediate) communication and coupling" – e.g. col. 3, lines 13-19 and in claim 15, "...the plurality of parsers each **coupled** to the event manager" and "...The system may include an event manager in communication with the event parser" – e.g. abstract) in communication with the central loghost over a network (Please see above 112 rejection. "Event parser 54 then streams the event object it has created to event manager 55..." – e.g. col. 6, lines 15-22. "System 10 is preferably a **web-based** platform...and is driven by **web-interface browsers** such as Netscape..and Internet Explorer...System 10 operates in conjunction with **a web server**" – e.g. col. 4, lines 11-20. Please note Khanolkar et al. further discloses in col. 1, lines 20-37, "..**computer communications networks**, especially **Internet-based networks**...". In other words, Internet communication system is the worldwide, publicly accessible network and **it would have been obvious to one of ordinary skill in the art** that an indirect communication through an intermediate communication disclosed in Khanolkar et al. can be the event parser is remote from the event manager within the same system communicated through Internet and an intermediate communication disclosed in Khanolkar et al. between event parser and event manager can be Internet since Khanolkar et al. reference discloses the system is a web-based and is driven by web-interface browsers and Internet is worldwide, publicly accessible network); and

at least one monitoring station ("event broadcaster 56" in fig. 2 corresponds to one monitoring station),

wherein the proxy loghost receives a plurality of log files (log data 18 in fig 1) from a plurality of resources (e.g. col. 3, lines 59- col. 4, line 2) operating on a network, analyzes the log files for at least one of unexpected volume, unexpected patterns ("a developing pattern of intrusion" – e.g. col. 4, lines 54-55. Please note the word "intrusion" should be broadly understood to include any type of security breach and accidental or inadvertent misuse as well as an actual intrusion disclosed in col. 3, lines 5-9. Therefore, it meets the claim limitation of unexpected patterns) or unexpected types of log files, and generates events in view of such analysis (col. 7, lines 47-53),

wherein the central loghost is operable to receive the events generated by the proxy loghost through the network ("Event parser 54 then streams the event object it has created to event manager 55..." – e.g. col. 6, lines 15-22. "System 10 is preferably a **web-based** platform...and is driven by **web-interface browsers** such as Netscape..and Internet Explorer...System 10 operates in conjunction with **a web server**" – e.g. col. 4, lines 11-20. Please note Khanolkar et al. further discloses in col. 1, lines 20-37, "..**computer communications networks**, especially **Internet-based networks**...) and generate an alert upon an analysis of the events, and wherein the monitoring station is caused to issue an alarm when the alert is generated (col. 7, lines 14-22 and col. 7, line 53 – col. 8, line 11)

Please also note on col. 2, lines 25-44, Khanolkar et al. discloses "the system has discrete software modules that receive and process log data from various network devices....". In light of the Applicant's specification in paragraph [0017] that both proxy

and central loghosts are independent modules and they can run on the same system. Therefore, the teachings of Khanolkar et al. met the limitations of the claim

As per **claim 2**, Khanolkar et al. discloses a system as applied in claim 1. Khanolkar et al. further discloses wherein the central loghost comprises a plurality modules operating in a Unix environment ("system 10 is preferably... implemented on ...Linux or Solaris server platforms..." –e.g. col. 4, lines 11-12).

Please note Linux is unix-like operating system and has unix background. Therefore, it met the limitation of the claim.

As per **claim 3**, Khanolkar et al. discloses a system as applied in claim 1. Khanolkar et al. further discloses comprising a plurality of proxy loghosts, each one of the plurality being in communication with the central loghost ("an event manager in communication with the event parser" – e.g. abstract and "a plurality of event parsers" – e.g. col. 7, lines 46—54).

As per **claim 4**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer (e.g. col. 3, lines 59 – col. 4, line 1).

As per **claim 5**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein a plurality of events is required to cause the generation of an alert ("It is also contemplated that a user may set no threshold...and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3)

As per **claim 6**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. met the limitation of claim 6 by further disclose wherein security management has access to both the proxy loghost and the central loghost ("....In event manager 55, as well as in other system modules and features, filter settings may be set by a user, for instance, a network administrator through web client interface 30...Settings may be modified by a user during system 10 operation by further input into web client interface 30" – e.g. col. 6, lines 38-54)

As per **claim 7**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the log files are received from a network-based intrusion detection system (e.g. col. 2, lines 1-9)

As per **claim 9**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the log files are archived on the proxy loghost and the events are archived on the central loghost (col. 1, lines 54- 62, col. 7, lines 24-29 and col. 7, lines 24-31).

Please note that proxy loghost and central loghost are running on the system 10 of the Khanolkar et al. And the database to hold archived files are located in the database 58 within the system 10 in fig. 2. Therefore, the teaching of Khanolkar et al. met the limitation of the claim.

As per **claim 10**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses comprising software adapters to convert one format of a log file to another format ("...log data...are converted to event objects for processing and manipulation by the system..." –e.g. col. 2, lines 25-32).

As per **claim 11**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses comprising a module for visualizing the log files received at the proxy loghost ("system 10 operates in conjunction with a web server, such as Apache or Netscape" – e.g. col. 4, lines 14-15).

As per **claims 12 and 22**, Khanolkar et al. discloses a system/method, comprising:

a plurality of proxy loghosts ("discrete software modules" – e.g. col. 2, line 25), each proxy loghost collecting log files that are generated by resources in a portion of the secure network, the plurality of loghosts generating events in response to the log files collected (e.g. col. 2, lines 28-32); and

a central loghost remote from the plurality of proxy loghosts and in communication with the plurality of proxy loghosts over a network (Please see above 112 rejection and claim interpretation. "Event parser 54 then streams the event object it has created to event manager 55..." – e.g. col. 6, lines 15-22. "System 10 is preferably a **web-based** platform...and is driven by **web-interface browsers** such as Netscape..and Internet Explorer...System 10 operates in conjunction with **a web server**" – e.g. col. 4, lines 11-20. Please note Khanolkar et al. further discloses in col. 1, lines 20-37, "..**computer communications networks**, especially **Internet-based networks**...". In other words, internet and web are network as well. **It would have been obvious to one of ordinary skill in the art** that an indirect communication through an intermediate communication disclosed in Khanolkar et al. can be the event parser is remote from the event manager within the same system communicated through Internet and an intermediate communication disclosed in Khanolkar et al. between event parser and event manager can be Internet since Khanolkar et al. reference discloses the system is a web-based and is driven by web-interface browsers and Internet is worldwide, publicly accessible network), the central loghost receiving ~~at least one of (i)~~ the log files themselves and ~~(ii)~~ the events from the plurality of proxy loghosts, the central loghost analyzing the log files and the events (Please see above 112 rejection) to determine the necessity of generating an alert and an associated alarm to notify (col. 7, lines 14-22 and col. 7, line 53 – col. 8, line 11) a security manager ("a network security administrator or other network administrator" in col. 4, lines 44-45 corresponds to Applicant's security manager) of a possible intrusion incident.

As per **claims 13 and 23**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the central loghost comprises a plurality modules operating in a Unix environment ("system 10 is preferably...implemented on ...Linux or Solaris server platforms..." –e.g. col. 4, lines 11-12).

As per **claims 14 and 25**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer (e.g. col. 3, lines 59 – col. 4, line 1).

As per **claim 15**, Khanolkar et al. discloses a system as applied in claim 12. Khanolkar et al. further discloses wherein a plurality of events is required to cause the generation of an alert ("It is also contemplated that a user may set no threshold...and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3).

As per **claims 16 and 27**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein security management has access to both the plurality of proxy loghosts and the central loghost ("....In event manager 55, as well as in other system modules and features, filter settings may be set

by a user, for instance, a network administrator through web client interface 30... Settings may be modified by a user during system 10 operation by further input into web client interface 30" – e.g. col. 6, lines 38-54)

As per **claims 17 and 28**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the log files are received from a network-based intrusion detection system (e.g. col. 2, lines 1-9)

As per **claims 19 and 30**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the log files are archived on the plurality of proxy loghosts and events are archived on the central loghost (col. 1, lines 54- 62, col. 7, lines 24-29 and col. 7, lines 24-31).

Please note that proxy loghost and central loghost are running on the system 10 of the Khanolkar et al. And the database to hold archived files are located in the database 58 within the system 10 in fig. 2. Therefore, the teaching of Khanolkar et al. met the limitation of the claim.

As per **claim 20**, Khanolkar et al. discloses the system as applied in claim 12. Khanolkar et al. further discloses comprising software adapters to convert one format of a log file to another format ("... log data... are converted to event objects for processing and manipulation by the system..." –e.g. col. 2, lines 25-32).

As per **claim 21**, Khanolkar et al. discloses the system as applied in claim 12. Khanolkar et al. further discloses comprising a module for visualizing the log files received at the proxy loghost ("system 10 operates in conjunction with a web server, such as Apache or Netscape" – e.g. col. 4, lines 14-15).

As per **claim 24**, Khanolkar et al. discloses the method as applied in claim 22. Khanolkar et al. further discloses wherein a plurality of proxy loghosts receive log files (col. 7, lines 38-50).

As per **claim 26**, Khanolkar et al. discloses the method as applied in claim 22. Khanolkar et al. further discloses comprising generating the alert only after a plurality events are received ("Therefore, the determination of whether to broadcast the event object as an intrusion alarm is made nearly instantaneously upon receipt of the event object" – e.g. col. 7, lines 14-22 and "It is also contemplated that a user may set no threshold...and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3).

12. Claims 8, 18 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar et al. as applied to claims 1-7, 9-17, 19-28 and 30 above, and further in view of Admitted prior art disclosed on line 6 of paragraph [0030], on page 9 - line 2 on page 10 of the specification of the current application.

As per **claim 8**, Khanolkar et al. discloses the limitation in claim 1 above and also in col. 1, line 23, Khanolkar discloses "password attacks", which is a type of attack Host-based intrusion system usually detects. By admitting "to the extent..**host-based systems** have already been implemented" in par. [0030] and in par. [0004] of the instant application, "Serveral commercial tools have been made available to combat such attacks...**these tools** generally fall into one of two catergoires...and **host-based systems**...". The claim would have been obvious because with "While **these commercial tools may be useful** in some contexts" as admitted by the Applicant in par. [0004], as a person with ordinary skill has good reason to pursue the known options within his or her technical grasp. In turn, because the log files are received from a host-based intrusion detection system as claimed has the properties predicted by the Applicant's admitted prior art, it would have been obvious to receive log files from a host-based intrusion detection system. *See KSR, 82 USPQ2d at 1397.*

As per **claims 18 and 29**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22 and also in col. 1, line 23, Khanolkar discloses "password attacks", which is a type of attack Host-based intrusion system usually detects. By admitting "to the extent..**host-based systems** have already been implemented" in par. [0030] and in par. [0004] of the instant application, "Serveral commercial tools have been made available to combat such attacks...**these tools** generally fall into one of two catergoires...and **host-based systems**...". The claim would have been obvious because with "While **these commercial tools may be useful** in some contexts" as

admitted by the Applicant in par. [0004], as a person with ordinary skill has good reason to pursue the known options within his or her technical grasp. In turn, because the log files are received from a host-based intrusion detection system as claimed has the properties predicted by the Applicant's admitted prior art, it would have been obvious to receive log files from a host-based intrusion detection system. *See KSR, 82 USPQ2d at 1397.*

Response to Arguments

13. Applicant's arguments filed 16 May 2007 have been fully considered but they are not persuasive.

14. The Applicant's essential arguments are:

A. "...Applicant has amended independent claims 1 and 12 to recite that the system is a computer-implemented system. Applicant therefore respectfully submits that claims 1-21 are directed to statutory subject matter and requests withdrawal the rejection", the examiner respectfully disagrees.

First, the new limitation "a computer-implemented...system" is being recited in the preamble. The Applicant is reminded that a preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand

alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Second, for the sake of the argument, even if "a computer-implemented...system" is given its patentable weight, it is the examiner's position is that a computer can be reasonably interpreted to one of ordinary skill in the art as software. According to "The Authoritative Dictionary of IEEE Standards Term Seventh EDITION", "computer 2 (A) (software) A functional unit that can perform substantial computing...during a run. (B) (software) A functional programmable unit that consists of one or more associated processing units..without human intervention" on page 207.

Third, the applicant adds "...network" in the claim. However, according to "The Authoritative Dictionary of IEEE Standards Term Seventh EDITION", "network 3 (A) (software) An interconnected or interrelated group of nodes" on page 725.

Therefore, because of the above facts, the examiner maintains 35 USC § 101 rejections for claims 1-21.

B. Regarding Applicant's amendment/argument to the independent claims 1, 12 and 22, the examiner respectfully traversed the argument/amendment in the above 112 and 103 rejection.

C. Regarding Applicant's argument on dependent claims 2-11, 13-21 and 23-30 being allowable due to dependency on page 10 of the remark. However, because the arguments for the independent claims are traversed, the dependent claims are also not allowable. Further, for claim 9, the additional argument on page 10 is traversed due to 112 rejection above.

D. Regarding Applicant's argument on dependent claims 8, 18 and 29 on pages 10-11, the examiner respectfully disagrees.

First, because the arguments for the independent claims are traversed, the dependent claims are also not allowable.

Second, the additional arguments on pages 10-11 are traversed and please see above 103 rejection.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-

1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

2 August 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100